



U.S. Department of Justice

Federal Bureau of Investigation

Washington, D.C. 20535

September 26, 2003

RECEIVED

SEP 26 2003

FEDERAL COMMUNICATIONS COMMISSION  
OFFICE OF THE SECRETARY

**By Hand Delivery**

Ms. Marlene H. Dortch, Secretary  
Federal Communications Commission  
445 12th Street, S.W.  
Room TW-B204  
Washington, D.C. 20554

**Re: *Petition to Adopt Conditions to Authorizations and Licenses In the Matter of Global Crossing Ltd., Transferor, and GC Acquisition Limited, Transferee, Application for Consent to Transfer Control and Petition for Declaratory Ruling, IB Docket No. 02-286***

Dear Ms. Dortch:

Transmitted herewith, on behalf of the United States Department of Defense ("DoD"), Department of Homeland Security ("DHS"), Department of Justice ("DoJ"), and the Federal Bureau of Investigation ("FBI") (collectively "Executive Agencies") are an original and four copies of the "Petition to Adopt Conditions to Authorizations and Licenses" regarding the above-referenced matter.

Pursuant to the Application, filed with the FCC in IB Docket No. 02-286, the Executive Agencies have reviewed the national security, law enforcement and public safety issues pertaining to this matter. The Executive Agencies now respectfully request that the Federal Communication Commission accept this Petition, and advise the Commission that none of the Executive Agencies object to the Commission granting the authorizations requested by Global Crossing Ltd. in this matter, provided that the Commission condition the grant on compliance with the terms of the Agreement and the Condition to FCC Authorization reached by Global Crossing Ltd, GC Acquisition Limited, and Singapore Technologies Telemedia Pte Ltd, and the Executive Agencies (a copy of which is attached to the Petition).

Sincerely,

Patrick W. Kelley  
Office of the General Counsel  
935 Pennsylvania Ave., N.W., Room 7427  
Washington, D.C. 20535  
(202) 324-8067

Enclosures  
cc: Qualex International

014  
1533 11

Before the  
**FEDERAL COMMUNICATIONS COMMISSION**  
Washington, D.C. 20554

\_\_\_\_\_  
)  
)  
**In the Matter of:** )  
)

**Global Crossing Ltd.** )  
**(Debtor-in-Possession),** )

**Transferor,** )

**and** )

**GC Acquisition Limited,** )

**Transferee,** )

**Application for Consent to Transfer** )  
**Control and Petition for Declaratory Ruling** )  
\_\_\_\_\_ )

**RECEIVED**

SEP 26 2003

FEDERAL COMMUNICATIONS COMMISSION  
OFFICE OF THE SECRETARY

**IB Docket No. 02-286**

**To: The Commission**

**PETITION TO ADOPT CONDITIONS TO**  
**AUTHORIZATIONS AND LICENSES**

The Department of Justice ("DOJ") and the Federal Bureau of Investigation ("FBI"), with the concurrence of the Department of Homeland Security ("DHS") and the Department of Defense ("DOD") (hereinafter collectively referred to as the "Executive Agencies"), respectfully submit this Petition to Adopt Conditions to Authorizations and Licenses ("Petition"), pursuant to 47 C.F.R. § 1.41.

Through this Petition, the Executive Agencies hereby advise the Federal Communications Commission ("FCC" or "Commission") that they have no objection to the FCC granting the relief requested in the applications filed in the above-referenced matter (herein referred to as

“requested relief”), provided that the Commission conditions the grant of the requested relief on the compliance by Global Crossing Ltd. (Debtor-in-Possession) (“GCL”), GC Acquisition Limited (“New GX” and, together with GCL, “Applicants”), and Singapore Technologies Telemedia (“ST Telemedia”) with the terms of the Agreement (attached hereto as Exhibit 1) reached between the Applicants and ST Telemedia, on the one hand, and the Executive Agencies, on the other.

On May 13, 2003, GCL and New GX filed an amendment to their August 22, 2002 applications, reflecting that Hutchison Telecommunications Limited (“Hutchison Telecom”) had withdrawn as an investor and that ST Telemedia had assumed Hutchison Telecom’s rights and obligations in addition to maintaining the rights and obligations originally held by ST Telemedia pursuant to the purchase agreement. The August 22, 2002 applications, as amended in the May 13, 2003 filing and in other filings both before and after that date, seek Commission consent to transfer control of GCL’s FCC-licensed subsidiaries from GCL to New GX, and request a declaratory ruling that the proposed indirect ownership interest in Global Crossing North American Networks, Inc. and Equal Access Networks, LLC by ST Telemedia, a Singapore company, is in the public interest under section 310(b)(4) of the Communications Act.

**In their filings, the Applicants represented** that ST Telemedia proposes to invest \$250 million in New GX and to obtain a 61.5% controlling interest in New GX and the FCC-licensed subsidiaries. The pre-petition creditors of GCL and its debtor subsidiaries (the “Creditors”) would obtain a 38.5% equity interest in New GX. The interests of ST Telemedia and the Creditors would continue to be subject to dilution as a result of the contemplated issuance and exercise of stock options to the future management of New GX in an amount up to 8% of the

equity of New GX

As the Commission is aware, the DOJ, FBI and DOD have taken the position that their ability to satisfy their obligations to protect the national security, to enforce the laws and preserve the safety of the public could be significantly impaired by transactions in which foreign entities will own or operate a part of the U.S. communications system, or in which foreign-located facilities will be used to provide domestic communications services to U.S. customers. In such cases, the DOJ, FBI and DOD have stated that foreign involvement in the provision of U.S. communications must not be permitted to impair the U.S. government's ability to satisfy its obligations to U S citizens to (1) carry out lawfully-authorized electronic surveillance of domestic U S. calls or calls that originate or terminate in the United States; (2) prevent and detect foreign-based espionage and electronic surveillance of U S communications, activities which if allowed to occur undetected would jeopardize the security and privacy of U.S. communications and undermine prosecution of individuals involved in such activities, and (3) satisfy U.S. critical infrastructure protection requirements. To address these concerns, the DOJ, the FBI, and the DOD have entered into agreements with the appropriate parties. The agreements reached in the past have been filed by stipulation among the parties with the Commission, and the Commission has conditioned its grant of approvals of the requested transfers of control on compliance with the terms of the agreements.<sup>1</sup>

---

<sup>1</sup> See, e g , Memorandum Opinion and Order, *Merger of MCI Communications Corp and British Telecommunications, plc*, 12 FCC Rcd 15,351 (1997) (agreement adopted by the Commission, but the merger did not take place), Memorandum Opinion and Order, *AirTouch Communications, Inc and Vodafone Group, plc*, DA No. 99-1200, 1999 WL 413237 (rel. June 22, 1999), Memorandum Opinion and Order, *AT&T Corp , British Telecommunications, plc, VLT Co L L C , Violet License Co , LLC and TNV [Bahamas]*, 14 FCC Rcd (Oct 29, 1999); Memorandum Opinion and Order, *Vodafone AirTouch PLC and Bell Atlantic Corp* , DA No. 99-2415, 2000 WL

In their August 22, 2002 applications, the Applicants requested that action by the Commission be deferred pending notification to the Commission that any law enforcement, national security, and public safety issues identified by the Executive Agencies have or have not been resolved and requesting appropriate action by the Commission. The Applicants observed that, if the issues identified by the Executive Agencies can be resolved through an agreement between the Applicants and the Executive Agencies, the Applicants anticipated that such agreement would be filed with the Commission along with a request that the terms of the agreement be adopted by the Commission as conditions to any authority granted by the Commission concerning the applications. The parties were then in discussions to reach an agreement that would ensure that national security, law enforcement and public safety concerns are adequately addressed.

On October 21, 2002, the DOJ and the FBI filed a Motion for Continued Deferral, and in the Applicants' May 13, 2003 filing amending their initial applications, Applicants reiterated their request that the Commission defer dispositive action until the Commission receives notice from the Executive Agencies that any national security or law enforcement issues have been resolved and requesting appropriate action by the Commission

---

332670 (rel Mar 30, 2000), Memorandum Opinion and Order, *Aerial Communications, Inc and VoiceStream Wireless Holding Corp*, 15 FCC Rcd 10,089 (2000), Memorandum Opinion and Order, *DiGiPH PCS, Inc and Eliska Wireless Ventures License Subsidiary I, L L C*, No. 15639 (rel Dec 13, 2000), Memorandum Opinion and Order, *VoiceStream Wireless Corporation, Powertel, Inc , et al and Deutsche Telekom AG*, IB Docket No 00-187, 2001 WL 431689 (F.C.C.)(rel. April 27, 2001); Memorandum Opinion, Order and Authorization, *XO Communications, Inc*, 17 FCC Rcd 19,212, 2002 WL 31235646 (F.C.C.) (2002) (agreement adopted by the Commission, but the transaction was not consummated)

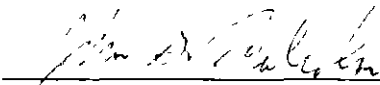
During the course of discussions between the DOJ, FBI, and DOD and the Applicants, the Department of Homeland Security assumed its responsibilities under the Homeland Security Act of 2002. In addition, by Executive Order dated March 1, 2003, the Secretary of Homeland Security became a member of the Committee on Foreign Investment in the United States. *See* the Defense Production Act, 50 U.S.C. App. § 2170. DHS thereafter joined the DOJ, FBI, and DOD in discussions with GCL, New GX, and ST Telemedia in connection with the proposed acquisition and transfers of control.

On September 24, 2003, the Executive Agencies entered into the Agreement with GCL, New GX, and ST Telemedia. The Agreement is intended to ensure that the Executive Agencies and other entities with responsibility for enforcing the law, protecting the national security and preserving public safety can proceed in a legal, secure and confidential manner to satisfy these responsibilities.

Accordingly, the DOJ and the FBI, with the concurrence of the DOD and DHS, hereby advise the Commission that they have no objection to the FCC granting the proposed transfers of control and petition for declaratory ruling in IB Docket No. 02-286, provided that the Commission conditions its consent to the transfer of control of New GX and grant of a declaratory ruling on compliance with the terms of the Agreement between the Executive Agencies, on the one hand, and GCL, New GX and ST Telemedia, on the other.

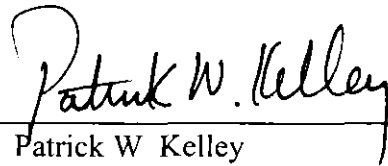
The DOJ and FBI are authorized to state that the Applicants and ST Telemedia do not object to the grant of this Petition.

Respectfully submitted,



---

John G. Malcolm  
Deputy Assistant Attorney General  
Criminal Division  
950 Pennsylvania Avenue, N.W.  
Washington, DC 20530  
(202) 616-3928



---

Patrick W. Kelley  
Deputy General Counsel  
Federal Bureau of Investigation  
935 Pennsylvania Avenue, N.W.  
Washington, DC 20532  
(202) 324-6829

September 26, 2003

### CERTIFICATE OF SERVICE

I, Myla R Saldivar-Trotter, hereby certify that on this 26<sup>th</sup> day of September, 2003, I caused a true and correct copy of the foregoing Petition to Adopt Conditions to Authorizations and Licenses to be served upon the following parties by hand-delivery (indicated by\*) or by United States Postal Service First-Class Mail

J. Breck Blalock\*  
Deputy Chief  
Policy Division  
International Bureau  
Federal Communications Commission  
445 12<sup>th</sup> Street, SW  
Washington, D C 20554

Susan O'Connell\*  
Policy Division  
International Bureau  
Federal Communications Commission  
445 12<sup>th</sup> Street, SW  
Washington, D.C 20554

Kathleen Collins\*  
Senior Legal Advisor  
Policy Division  
International Bureau  
Federal Communications Commission  
445 12<sup>th</sup> Street, SW  
Washington, D C 20554

Henry Thaggert\*  
Wireline Competition Bureau  
Federal Communications Commission  
445 12<sup>th</sup> Street, SW  
Washington, D C. 20554

Zenji Nakazawa\*  
Public Safety and Private Wireless Division  
Wireless Telecommunications Bureau  
Federal Communications Commission  
445 12<sup>th</sup> Street, SW  
Washington, D C 20554

Neil Dellar\*  
Office of the General Counsel  
Federal Communications Commission  
445 12<sup>th</sup> Street, SW  
Washington, D.C 20554

James Ball\*  
Chief  
Policy Division  
International Bureau  
Federal Communications Commission  
445 12<sup>th</sup> Street, SW  
Washington, D C 20554

William Malone, Esq.  
Gerald Lavery Lederer, Esq  
James R. Hobson, Esq.  
Miller & Van Eaton, PLLC  
1155 Connecticut Avenue, NW  
Suite 1000  
Washington, D C 20036-4320

Debbie Goldman  
Louise Novotny  
Communications Workers of America  
501 3rd St., N W  
Washington, D C 20001-2797

Karl W. B. Schwarz  
CommAxxess  
310 W. St. Louis  
Hot Springs, AK 71913

Mark Tauber, Esq  
E Ashton Johnston, Esq  
Piper Rudnick LLP  
1200 Nineteenth Street, NW  
Washington, DC 20036

Todd Malan  
Organization for International Investment  
1901 Pennsylvania Avenue, NW  
Suite 807  
Washington, D.C 20006



Douglas W Kinkoph  
Christopher T McKee  
XO Communications, Inc  
11111 Sunset Hills Road  
Reston, VA 20190

Jean L Kiddoo  
Paul O Gagnier  
Swidler Berlin Shereff Friedman, LLP  
3000 K Street N W , Suite 300  
Washington, D C 20007

Cheryl A. Trutt  
Joan E. Neal  
Morrison & Foerster LLP  
2000 Pennsylvania Avenue, NW  
Suite 5500  
Washington, D C 20006-1888

Teresa D Baer, Esq  
Latham & Watkins LLP  
555 Eleventh Street, NW  
Suite 1000  
Washington, D.C 20004

  
Myla R. Saldivar-Trotter

## **AGREEMENT**

This AGREEMENT is made as of the date of the last signature affixed hereto by and among Global Crossing Ltd ("GCL"), GC Acquisition Limited ("New GX") and Singapore Technologies Telemedia Pte Ltd ("ST Telemedia"), on the one hand, and the Federal Bureau of Investigation ("FBI"), the U S Department of Justice ("DOJ"), the Department of Defense ("DOD"), and the Department of Homeland Security ("DHS"), on the other (referred to individually as a "Party" and collectively as the "Parties")

## **RECITALS**

**WHEREAS**, U S communication systems are essential to the ability of the U S government to fulfill its responsibilities to the public to preserve the national security of the United States, to enforce the laws, and to maintain the safety of the public;

**WHEREAS**, the U S government has an obligation to the public to ensure that U.S. communications and related information are secure in order to protect the privacy of U.S. persons and to enforce the laws of the United States,

**WHEREAS**, it is critical to the well being of the nation and its citizens to maintain the viability, integrity, and security of the communications systems of the United States (*see, e.g.*, Executive Order 13231, Critical Infrastructure Protection in the Information Age and Presidential Decision Directive 63, Critical Infrastructure Protection);

**WHEREAS**, protection of Classified, Controlled Unclassified, and Sensitive Information is also critical to U S national security,

**WHEREAS**, GCL and New GX have an obligation to protect from unauthorized disclosure the contents of wire and electronic communications;

**WHEREAS**, New GX, through one or more of its subsidiaries, provides or will provide the following services (1) local, long distance and international voice services including IP-based voice services, calling card and toll free voice service, and international toll free service, (2) private data and virtual private networking services, including global ATM service, and frame relay service, (3) broadband fiber-optic capacity on a leased and IRU basis, including private line service and wavelength service, (4) Internet access services including IP peering and transit service, dedicated Internet access service and internet dial-up service; (5) audio and video conferencing services, (6) maintenance and installation services in connection with the above, including colocation service, remote access service and managed services, and (7) any other telecommunications service that New GX may offer in the future,

**WHEREAS**, New GX has or will have direct physical or electronic access to certain customer facilities, including servers, storage media, network connections, bandwidth transport, and firewalls, and thereby has access to a variety of customer and end-user information that is subject to U S privacy and electronic surveillance laws,

**WHEREAS**, GCL has entered into a Purchase Agreement dated August 9, 2002 and amended December 20, 2002 and May 13, 2003 (the "Purchase Agreement"), whereby GCL and its wholly-owned Bermuda subsidiary, Global Crossing Holdings, Ltd., will transfer all of their assets and operations, including ownership of their U.S. subsidiaries, to New GX, and ST Telemedia will acquire, directly or through a subsidiary, a 61.5 percent equity and voting interest in New GX in exchange for, *inter alia*, an investment of \$250 million in New GX, which Purchase Agreement has been approved by the United States Bankruptcy Court for the Southern District of New York, and GCL, New GX and ST Telemedia have represented that the proposed transaction does not involve, directly or indirectly, investment in GCL, its subsidiaries, assets and operations by any foreign company other than ST Telemedia,

**WHEREAS**, GCL and New GX have filed with the Federal Communications Commission ("FCC") applications (in FCC IB Docket No. 02-286) under Sections 214 and 310(d) of the Communications Act of 1934, as amended (the "1996 Act"), 47 U.S.C. §§ 214 and 310(d), and the Act Relating to the Landing and Operation of Submarine Cables in the United States, as amended (the "Cable Landing License Act"), 47 U.S.C. §§ 34-39, seeking FCC approval of the transfer of control to New GX of GCL's subsidiaries that hold FCC authorizations and licenses, and in connection therewith have also filed with the FCC a petition pursuant to Section 310(b)(4) of the 1996 Act for a declaratory ruling that the proposed indirect foreign ownership interest of ST Telemedia in the FCC-licensed subsidiaries is in the public interest,

**WHEREAS**, ST Telemedia is a company organized and existing under the laws of Singapore that is a wholly-owned subsidiary of Singapore Technologies Pte Ltd, that in turn ultimately is wholly-owned by the government of the Republic of Singapore;

**WHEREAS**, the FCC's grant of the applications in FCC IB Docket No. 02-286 may be made subject to conditions relating to national security, law enforcement, and public safety, and whereas GCL, New GX and ST Telemedia have agreed to enter into this Agreement with the FBI, the DOJ, the DOD and the DHS to address issues raised by those departments and agencies and to request that the FCC condition the transfer of control approved by the FCC on their compliance with this Agreement,

**WHEREAS**, by Executive Order 12661, the President, pursuant to Section 721 of the Defense Production Act, as amended, authorized the Committee on Foreign Investment in the United States ("CFIUS") to review, for national security purposes, foreign acquisitions of U.S. companies,

**WHEREAS**, GCL, New GX and ST Telemedia have submitted a voluntary notice to CFIUS regarding ST Telemedia's proposed investment in New GX, and GCL, New GX and ST Telemedia have entered into this Agreement to resolve any national security issues that the DOJ, the FBI, the DOD and the DHS might raise, including in the CFIUS review process; and

**WHEREAS**, representatives of GCL, New GX and ST Telemedia have met with representatives of the FBI, the DOJ, the DOD and the DHS to discuss issues raised by those departments and agencies. In these meetings, GCL, New GX, and ST Telemedia represented that (a) they have no present plans, and are not aware of present plans of any other entity, that

would result in a Domestic Communications Company providing Domestic Communications through facilities located outside the United States, except as otherwise provided in Section 2.1 of this Agreement, (b) ST Telemedia is an entity whose commercial operations are wholly separate from the government of the Republic of Singapore and whose activities are overseen by independent regulatory authorities in Singapore, (c) no government has or will have, as a direct or indirect shareholder of New GX, special voting or veto rights concerning the actions of New GX, and GCL and New GX are aware of no plans the result of which would confer special voting or veto rights to any government, and (d) except as otherwise provided in Section 3.22, there are no present plans, and GCL and New GX are aware of no present plans of any other entity, as a result of which GCL or New GX will provide, direct, control, supervise or manage Domestic Communications through facilities located outside the United States

**NOW THEREFORE**, the Parties are entering into this Agreement to address national security, law enforcement and public safety issues

## **ARTICLE 1: DEFINITION OF TERMS**

As used in this Agreement

1.1 “Call Associated Data” means any information related to a Domestic Communication or related to the sender or recipient of that Domestic Communication and, to the extent maintained by a Domestic Communications Company in the normal course of business, includes without limitation subscriber identification, called party number, calling party number, start time, end time, call duration, feature invocation and deactivation, feature interaction, registration information, user location, diverted to number, conference party numbers, post cut-through dial digit extraction, in-band and out-of-band signaling, and party add, drop and hold.

1.2 “Classified Information” means any information that has been determined pursuant to Executive Order 12958, or any predecessor or successor order, or the Atomic Energy Act of 1954, or any statute that succeeds or amends the Atomic Energy Act, to require protection against unauthorized disclosure

1.3 “Control” and “Controls” means the power, direct or indirect, whether or not exercised, and whether or not exercised or exercisable through the ownership of a majority or a dominant minority of the total outstanding voting securities of an entity, or by proxy voting, contractual arrangements, or other means, to determine, direct, or decide matters affecting an entity, in particular, but without limitation, to determine, direct, take, reach, or cause decisions regarding.

- (i) the sale, lease, mortgage, pledge, or other transfer of any or all of the principal assets of the entity, whether or not in the ordinary course of business;
- (ii) the dissolution of the entity,
- (iii) the closing and/or relocation of the production or research and development facilities of the entity,

- (iv) the termination or nonfulfillment of contracts of the entity,
- (v) the amendment of the articles of incorporation or constituent agreement of the entity with respect to the matters described in subsections (i) through (iv) above; or
- (vi) New GX's and GCL's obligations under this Agreement.

1 4        "Controlled Unclassified Information" means unclassified information, the export of which is controlled by the International Traffic in Arms Regulations (ITAR), 22 C.F.R. Chapter I, Subchapter M, or the Export Administration Regulations (EAR), 15 C.F.R., Chapter VII, Subchapter C

1 5        "De facto" and "de jure" control have the meanings provided in 47 C F R §  
1 2110

1 6        "DHS" means the U S Department of Homeland Security

1 7        "DOD" means the U S Department of Defense

1 8        "DOJ" means the U S Department of Justice.

1 9.        "Domestic Communications" means (i) Wire Communications or Electronic Communications (whether stored or not) from one U S location to another U S location and (ii) the U S portion of a Wire Communication or Electronic Communication (whether stored or not) that originates or terminates in the United States

1 10        "Domestic Communications Company" means all those subsidiaries, divisions, departments, branches, other components of New GX and any other entity over which New GX has *de facto* or *de jure* control that provide Domestic Communications. If any subsidiary, division, department, branch, other component of New GX or any other entity over which New GX has *de facto* or *de jure* control provides Domestic Communications after the date that all the Parties execute this Agreement, then such entity shall be deemed to be a Domestic Communications Company. If any Domestic Communications Company enters into joint ventures under which a joint venture or another entity may provide Domestic Communications, and if a Domestic Communications Company has the power or authority to exercise *de facto* or *de jure* control over such entity, then New GX will ensure that entity shall fully comply with the terms of this Agreement. The term "Domestic Communications Company" shall not include acquisitions by New GX in the U.S. after the date this Agreement is executed by all parties only if the DOJ, FBI, DOD and DHS find that the terms of this Agreement are inadequate to address national security, law enforcement or public safety concerns presented by that acquisition and the necessary modifications to this Agreement cannot be reached pursuant to Section 8 10 below. Nothing in this definition shall exempt any Domestic Communications Company from its obligations under Section 5 3

1 11        "Domestic Communications Infrastructure" means (a) transmission, switching, bridging and routing equipment (including software and upgrades) subject to control by a

Domestic Communications Company and in use to provide, process, direct, control, supervise or manage Domestic Communications, and (b) facilities and equipment in use by or on behalf of a Domestic Communications Company that are physically located in the United States, or (c) facilities in use by or on behalf of a Domestic Communications Company to control the equipment described in (a) and (b) above. Domestic Communications Infrastructure does not include equipment or facilities used by service providers that are not Domestic Communications Companies and that are:

- (i) interconnecting communications providers; or
- (ii) providers of services or content that are
  - (A) accessible using the communications services of Domestic Communications Companies, and
  - (B) available in substantially similar form and on commercially reasonable terms through communications services of companies other than Domestic Communications Companies

Domestic Communications Infrastructure does not include equipment dedicated to the termination of international undersea cables, provided that such equipment is utilized solely to effectuate the operation of undersea transport network(s) outside of the United States and in no manner controls land-based transport network(s) or their associated systems in the United States

1 12 “Effective Date” means the date on which the transactions contemplated by the Purchase Agreement are consummated

1 13 “Electronic Communication” has the meaning given it in 18 U.S.C. § 2510(12).

1 14 “Electronic Surveillance” means: (a) the interception of wire, oral, or electronic communications as defined in 18 U.S.C. §§ 2510(4), (1), (2), and (12), respectively, and electronic surveillance as defined in 50 U.S.C. § 1801(f); (b) access to stored wire or electronic communications, as referred to in 18 U.S.C. § 2701 *et seq.*, (c) acquisition of dialing, routing, addressing or signaling information through pen register or trap and trace devices or other devices or features capable of acquiring such information pursuant to law as defined in 18 U.S.C. § 3121 *et seq.* and 50 U.S.C. § 1841 *et seq.*, (d) acquisition of location related information concerning a service subscriber or facility; (e) preservation of any of the above information pursuant to 18 U.S.C. § 2703(f); and (f) access to, or acquisition or interception of, or preservation of communications or information as described in (a) through (e) above and comparable State laws

1 15. “FBI” means the Federal Bureau of Investigation.

1 16 “Foreign” where used in this Agreement, whether capitalized or lower case, means non-U.S.

1 17 “GCL” means Global Crossing Ltd., a Bermuda corporation

1.18 “Governmental Authority” or “Governmental Authorities” means any government, or any governmental, administrative, or regulatory entity, authority, commission, board, agency, instrumentality, bureau, or political subdivision, and any court, tribunal, judicial, or arbitral body

1.19 “Intercept” or “Intercepted” has the meaning defined in 18 U.S.C. § 2510(4)

1.20 “Lawful U.S. Process” means lawful U.S. Federal, state, or local Electronic Surveillance or other court orders, processes, or authorizations issued under U.S. Federal, state, or local law for physical search or seizure, production of tangible things, or access to or disclosure of Domestic Communications or Call Associated Data, including Transactional Data or Subscriber Information

1.21 “Network Management Information” means network management operations plans, processes and procedures, the placement of Network Operating Center(s) and linkages (for service off load or administrative activities) to other domestic and international carriers, ISPs and other critical infrastructures, descriptions of IP networks and operations processes and procedures for management control and relation to the backbone infrastructure(s) including other service providers, description of any unique/proprietary control mechanisms as well as operating and administrative software, and network performance information

1.22 “New GX” means GC Acquisition Limited, a Bermuda corporation, and its subsidiaries and affiliates

1.23 “New GX Board” means the board of directors of New GX.

1.24 “OPM” means the Office of Personnel Management of the U.S. Government

1.25 “Party” and “Parties” have the meanings given them in the Preamble.

1.26 “Pro forma assignments” or “pro forma transfers of control” are transfers that do not involve a substantial change in ownership or control as provided by the FCC’s Rules

1.27 “Purchase Agreement” has the meaning given in the Recitals

1.28 “Security Committee” means a committee of the New GX Board the mandate of which is to oversee security matters and implementation of this Agreement within New GX

1.29 “Security Director” has the meaning given in Section 3.15

1.30 “Security Officer” has the meaning given in Sections 3.10 and 3.13.

1.31 “Sensitive Information” means information that is not Classified Information regarding (a) the persons or facilities that are the subjects of Lawful U.S. Process, (b) the identity of the government agency or agencies serving such Lawful U.S. Process, (c) the location or identity of the line, circuit, transmission path, or other facilities or equipment

used to conduct Electronic Surveillance pursuant to Lawful U.S. Process, (d) the means of carrying out Electronic Surveillance pursuant to Lawful U.S. Process, (e) the type(s) of service, telephone number(s), records, communications, or facilities subjected to Lawful U.S. Process, (f) information deemed to be Sensitive Information pursuant to Executive Order, decision or guidelines, and (g) other information that is not Classified Information designated in writing by an authorized official of a Federal, state or local law enforcement agency or a U.S. intelligence agency as "Sensitive Information." Domestic Communications Companies may dispute pursuant to Article 4 whether information is Sensitive Information under this subparagraph. Such information shall be treated as Sensitive Information unless and until the dispute is resolved in the Domestic Communications Companies' favor.

1 32     "ST Telemedia" has the meaning given in the Preamble.

1 33     "Subscriber Information" means information relating to subscribers or customers of Domestic Communications Companies of the type referred to and accessible subject to procedures specified in 18 U.S.C. § 2703(c) or (d) or 18 U.S.C. § 2709. Such information shall also be considered Subscriber Information when it is sought pursuant to the provisions of other Lawful U.S. Process.

1 34     "Transactional Data" means

- (i) "call identifying information," as defined in 47 U.S.C. § 1001(2), including without limitation the telephone number or similar identifying designator associated with a Domestic Communication,
- (ii) any information possessed by a Domestic Communications Company relating specifically to the identity and physical address of a customer or subscriber, or account payer, or the end-user of such customer or subscriber, or account payer, or associated with such person relating to all telephone numbers, domain names, IP addresses, Uniform Resource Locators ("URLs"), other identifying designators, types of services, length of service, fees, usage including billing records and connection logs, and the physical location of equipment, if known and if different from the location information provided under (iv) below;
- (iii) the time, date, size or volume of data transfers, duration, domain names, MAC or IP addresses (including source and destination), URLs, port numbers, packet sizes, protocols or services, special purpose flags, or other header information or identifying designators or characteristics associated with any Domestic Communication, and
- (iv) as to any mode of transmission (including mobile transmissions), and to the extent permitted by U.S. laws, any information indicating as closely as possible the physical location to or from which a Domestic Communication is transmitted



The term includes all records or other information of the type referred to and accessible subject to procedures specified in 18 U.S.C § 2703(c)(1) and (d), but does not include the content of any communication

1 35. “United States,” “US,” or “U S” means the United States of America including all of its States, districts, territories, possessions, commonwealths, and the special maritime and territorial jurisdiction of the United States

1 36 “Wire Communication” has the meaning given it in 18 U.S.C § 2510(l)

1 37 Other Definitional Provisions Other capitalized terms used in this Agreement and not defined in this Article shall have the meanings assigned them elsewhere in this Agreement. The definitions in this Agreement are applicable to the singular as well as the plural forms of such terms and to the masculine as well as to the feminine and neuter genders of such term. Whenever the words “include,” “includes,” or “including” are used in this Agreement, they shall be deemed to be followed by the words “without limitation.”

## **ARTICLE 2: FACILITIES, INFORMATION STORAGE AND ACCESS**

2 1 Domestic Communications Infrastructure Except to the extent and under conditions concurred in by the FBI, DOJ, DOD, and DHS in writing

- (i) all Domestic Communications Infrastructure that is owned, operated or controlled by a Domestic Communications Company shall at all times be located in the United States and will be directed, controlled, supervised and managed by a Domestic Communications Company; and
- (ii) all Domestic Communications that are carried by or through, in whole or in part, the Domestic Communications Infrastructure shall pass through a facility under the control of a Domestic Communications Company and physically located in the United States, from which Electronic Surveillance can be conducted pursuant to Lawful U.S. Process. The Domestic Communications Company will provide technical or other assistance to facilitate such Electronic Surveillance.
- (iii) foreign connections to the domestic Global Crossing network shall be on a gateway basis using industry best practices (i.e., both signaling and traffic shall be monitored for unauthorized access, network intrusions and other malicious activity). Such practices will be jointly determined by New GX and the FBI, DOJ, DOD and DHS.

2 2 Compliance with Lawful U.S. Process Domestic Communications Companies shall take all practicable steps to configure their Domestic Communications Infrastructure to be capable of complying, and Domestic Communications Company employees in the United States will have unconstrained authority to comply, in an effective, efficient, and unimpeded fashion, with

- (i) Lawful U.S. Process,

- (ii) the orders of the President in the exercise of his/her authority under § 706 of the Communications Act of 1934, as amended, 47 U.S.C. § 606, and under § 302(e) of the Aviation Act of 1958, 49 U.S.C. § 40107(b) and Executive Order 11161 (as amended by Executive Order 11382), and
- (iii) National Security and Emergency Preparedness rules, regulations and orders issued pursuant to the Communications Act of 1934, as amended, 47 U.S.C. § 151 *et seq*

2.3 Information Storage and Access. Domestic Communications Companies shall store exclusively in the United States the following:

- (i) stored Domestic Communications, if such communications are stored by or on behalf of a Domestic Communications Company for any reason,
- (ii) any Wire Communications or Electronic Communications (including any other type of wire, voice or electronic communication not covered by the definitions of Wire Communication or Electronic Communication) received by, intended to be received by, or stored in the account of a customer or subscriber of a Domestic Communications Company, if such communications are stored by or on behalf of a Domestic Communications Company for any reason,
- (iii) Transactional Data and Call Associated Data relating to Domestic Communications, if such data are stored by or on behalf of a Domestic Communications Company for any reason;
- (iv) Subscriber Information, if such information is stored by or on behalf of a Domestic Communications Company for any reason, concerning customers who are U.S.-domiciled, customers who hold themselves out as being U.S.-domiciled, and customers who make a Domestic Communication;
- (v) billing records of customers who are U.S.-domiciled, customers who hold themselves out as being U.S.-domiciled, and customers who make a Domestic Communication, for so long as such records are kept and at a minimum for as long as such records are required to be kept pursuant to applicable U.S. law or this Agreement, and
- (vi) Network Management Information

2.4 Billing Records. Domestic Communications Companies shall store for at least 18 months all billing records described in Section 2.3(v) above. Nothing in this paragraph shall require a Domestic Communications Company to store such records for longer than 18 months.

2.5 Storage Pursuant to 18 U.S.C. § 2703(f) Upon a request made pursuant to 18 U.S.C. § 2703(f) by a Governmental Authority in the United States to preserve any information in the possession, custody, or control of Domestic Communications Companies

that is enumerated in Section 2.3 above, Domestic Communications Companies shall store such information in the United States

2.6 Compliance with U.S. Law Nothing in this Agreement shall excuse a Domestic Communications Company from any obligation it may have to comply with U.S. legal requirements for the retention, preservation, or production of such information or data. Similarly, in any action to enforce Lawful U.S. Process, Domestic Communication Companies have not waived any legal right they might have to resist such process

2.7 Routing of Domestic Communications. Except for routing of traffic (i) to U.S. states, territories and possessions outside the Continental United States, (ii) to avoid network disruptions, (iii) consistent with least-cost routing practices that are implemented pursuant to policies reviewed and approved by the third-party auditor selected pursuant to Section 5.8 of this Agreement, and (iv) as otherwise may be agreed by the DOJ, the FBI, DOD and the DHS, Domestic Communications Companies shall not route Domestic Communications outside the United States

2.8 Interconnection Arrangements with ST Telemedia and Subsidiaries Interconnection arrangements between Domestic Communications Companies, on the one hand, and ST Telemedia and its subsidiaries, on the other hand, shall be on an arms' length basis

2.9 CPNI Domestic Communications Companies shall comply, with respect to Domestic Communications, with all applicable FCC rules and regulations governing access to and storage of Customer Proprietary Network Information ("CPNI"), as defined in 47 U.S.C. § 222(h)(1).

2.10 Storage of Protected Information The storage of Classified, Controlled Unclassified, and Sensitive Information by a Domestic Communications Company or its contractors at any location outside of the United States is prohibited, unless the storage is at a U.S. military facility, a U.S. Embassy or Consulate or other location occupied by a U.S. government organization

2.11 Network Topography No later than 30 days after the Effective Date of this Agreement, New GX will provide to the FBI, DOJ, DHS and DOD a comprehensive description of the New GX domestic telecommunications network to include location of servers, routers, switches, operational systems software, and network security appliances and software

### ARTICLE 3: SECURITY

3.1 Measures to Prevent Improper Use or Access Domestic Communications Companies shall take all reasonable measures to prevent the use of or access to the Domestic Communications Infrastructure to conduct Electronic Surveillance, or to obtain or disclose Domestic Communications, Classified Information, Sensitive Information, or Controlled Unclassified Information, in violation of any U.S. Federal, state, or local laws or the terms of this Agreement. These measures shall include creating and complying with

detailed technical, organizational, operational, and personnel controls, policies and written procedures, necessary implementation plans, and physical security measures

3.2 Visitation Policy No later than ninety (90) days after the Effective Date, New GX shall adopt and implement a visitation policy for Domestic Communications Companies, for all visits to Domestic Communications Infrastructure. New GX will consult with DOJ, DHS and DOD on the design and implementation of its visitation policy. The visitation policy shall differentiate between categories of visits based on the sensitivity of the information, equipment and personnel to which the visitors will have access. The visitation policy shall require that:

- (i) the Security Officer shall review and approve or disapprove requests for visits to Domestic Communications Infrastructure (provided that, with respect to carrier hotels and other shared facilities, this policy will apply solely to the portion of the facility controlled by New GX) by all non-U.S. persons, organizations and entities. The Security Officer shall approve or deny visit requests on the basis of their compliance with the visitation policy; the Security Officer may specifically deny any visit request on security or related grounds, which grounds will be described more fully in the visitation policy.
- (ii) a written request for approval of a visit must be submitted to the Security Officer no less than seven (7) days prior to the date of the proposed visit. If a written request cannot be provided within seven (7) days of the proposed visit because of an unforeseen exigency, the request may be communicated via telephone to the Security Officer and immediately confirmed in writing; however, the Security Officer may refuse to accept any request submitted less than seven (7) days prior to the date of such proposed visit if the Security Officer determines that there is insufficient time to consider the request.
- (iii) the exact purpose and justification for the visit must be set forth in detail sufficient to enable the Security Officer to make an informed decision concerning the appropriateness of the proposed visit, and the Security Officer may refuse to accept any request that he or she believes lacks sufficient information. Each proposed visit and each individual visitor must be justified and a separate approval request must be submitted for each visit.
- (iv) the Security Officer evaluate the request as soon as practicable after receiving it. The Security Officer may approve or disapprove the request pending submittal of additional information by the requester. When practicable, the Security Officer's decision shall be communicated to the requester by any means at least one (1) day prior to the date of the proposed visit, and, in all cases, the decision shall be confirmed in writing as promptly as possible.
- (v) a record of all such visit requests, including the decision to approve or disapprove, and information regarding consummated visits, such as date and place, as well as the names, business affiliation and dates of birth of the visitors, and New GX personnel involved, be maintained by the Security Officer. In

addition, a chronological file of all documentation associated with such visits, together with records of approvals and disapprovals, shall be maintained for two (2) years by the Security Officer for provision at the request of the third party auditor identified pursuant to Section 5 8 below, or of the DOJ, FBI, DOD or DHS

- (vi) visitors be escorted at all times by an employee, and within conditions, including appropriate restrictions on access, set forth by the Security Officer that are commensurate with the place and purpose of the visit

The parties may agree in the visitation policy that certain visits of a routine and nonsensitive nature are exempt from one or more of the requirements above.

3 3 Records of Communications with Non-U.S. Citizens and Non-U.S. Entities New GX shall maintain a full and complete record of every electronic or written communication by the New GX directors, officers, employees and agents, with ST Telemedia directors, officers, employees and agents (including the names, business affiliations, and substance of the communications) that are related to interconnection agreements, Security Procedures and Policy, as well as major equipment purchases outlined in section 3.18, and Joint Venture provisions outlined in section 5 3, relating to Domestic Communications Companies. These records shall be maintained for a period of five (5) years by the Security Officer for provision at the request of the third party auditor identified pursuant to Section 5 8 below, or of the DOD, DOJ, FBI or DHS

3 4 Access by Foreign Government Authority. Domestic Communications Companies shall not, directly or indirectly, disclose or permit disclosure of, or provide access to Domestic Communications, Call Associated Data, Transactional Data, or Subscriber Information stored by Domestic Communications Companies to any person if the purpose of such access is to respond to the legal process or the request of or on behalf of a foreign government, identified representative, component or subdivision thereof without the express written consent of the DOJ or the authorization of a court of competent jurisdiction in the United States. Any such requests or submission of legal process described in this Section 3 4 of this Agreement shall be reported to the DOJ as soon as possible and in no event later than five (5) business days after such request or legal process is received by and known to the Security Officer. Domestic Communications Companies shall take reasonable measures to ensure that the Security Officer will promptly learn of all such requests or submission of legal process described in this Section 3.4 of this Agreement.

3 5 Disclosure to Foreign Government Authorities. Domestic Communications Companies shall not, directly or indirectly, disclose or permit disclosure of, or provide access to:

- (i) Classified, Sensitive, or Controlled Unclassified Information, or

- (ii) Subscriber Information, Transactional Data or Call Associated Data, including a copy of any Wire Communications or Electronic Communication, intercepted or acquired pursuant to Lawful U S Process

to any foreign government, identified representative, component or subdivision thereof without satisfying all applicable U S Federal, state and local legal requirements pertinent thereto, and obtaining the express written consent of the DOJ or the authorization of a court of competent jurisdiction in the United States. Any requests or any legal process submitted by a foreign government, an identified representative, a component or subdivision thereof to Domestic Communications Companies for the communications, data or information identified in this Section 3.5 of this Agreement that is maintained by Domestic Communications Companies shall be referred to the DOJ as soon as possible and in no event later than five (5) business days after such request or legal process is received by and known to the Security Officer unless the disclosure of the request or legal process would be in violation of an order of a court of competent jurisdiction within the United States. Domestic Communications Companies shall take reasonable measures to ensure that the Security Officer will promptly learn of all such requests or submission of legal process described in this Section 3.5.

3.6 Notification of Access or Disclosure Requests from Foreign Non-Governmental Entities Within ninety (90) days of receipt, Domestic Communications Companies shall notify DOJ in writing of legal process or requests by foreign nongovernmental entities to Domestic Communications Companies for access to or disclosure of Domestic Communications unless the disclosure of the legal process or request would be in violation of an order of a court of competent jurisdiction within the United States.

3.7 Security of Lawful U.S. Process Domestic Communications Companies shall protect the confidentiality and security of all Lawful U S. Process served upon them and the confidentiality and security of Classified, Sensitive, and Controlled Unclassified Information in accordance with U S Federal and state law or regulation and this Agreement. Information concerning Lawful U S Process, Classified Information, Sensitive Information, or Controlled Unclassified Information shall be under the custody and control of the Security Officer.

3.8 Points of Contact Within fourteen (14) days after the Effective Date, Domestic Communications Companies shall designate in writing to the FBI, DOJ, DOD and DHS at least three nominees already holding U S. security clearances, or who are eligible to receive such clearances and whose applications for such clearances have been submitted to DOD, to serve as a primary and two secondary points of contact within the United States with the authority and responsibility for accepting and overseeing the carrying out of Lawful U.S. Process. The points of contact shall be assigned to Domestic Communications Companies' office(s) in the United States, shall be available twenty-four (24) hours per day, seven (7) days per week and shall be responsible for accepting service and maintaining the security of Classified, Sensitive, and Controlled Unclassified Information and any Lawful U.S. Process in accordance with the requirements of U.S. law and this Agreement. Promptly after designating such points of contact, Domestic Communications Companies shall notify the FBI, DOJ, DOD and DHS in writing of the points of contact, and thereafter shall promptly

notify the FBI, DOJ, DOD and DHS of any change in such designation. The points of contact shall be resident U S citizens who hold U S security clearances (which may include interim security clearances), as outlined in Executive Order 12968, and shall serve as points of contact for new Domestic Communications Companies unless and until the FBI, DOJ, DOD and DHS are notified of any change in designation. Domestic Communications Companies shall cooperate with any request by a Government Authority within the United States that a background check and/or security clearance process be completed for a designated point of contact.

3.9 Information Security Plan Domestic Communications Companies shall develop, document, implement, and maintain an information security plan to:

- (i) maintain appropriately secure facilities (e.g., offices) within the United States for the handling and storage of any Classified, Sensitive or Controlled Unclassified Information,
- (ii) take appropriate measures to prevent unauthorized access to data or facilities that might contain Classified, Sensitive, or Controlled Unclassified Information;
- (iii) assign U S citizens to positions for which screening is contemplated pursuant to Section 3.12,
- (iv) upon request from the DOJ, FBI, DOD or DHS, provide the name, social security number and date of birth of each person who regularly handles or deals with Sensitive Information,
- (v) require that personnel handling Classified Information shall have been granted appropriate security clearances pursuant to Executive Order 12968;
- (vi) provide that the points of contact described in Section 3.8 of this Agreement shall have sufficient authority over any of Domestic Communications Companies' employees who may handle Classified, Sensitive, or Controlled Unclassified Information to maintain the confidentiality and security of such information in accordance with applicable U S legal authority and the terms of this Agreement,
- (vii) ensure that the disclosure of or access to Classified, Sensitive, or Controlled Unclassified Information is limited to those who have the appropriate security clearances and authority,
- (viii) establish a formal incident response capability with reference to OMB Circular A-130 and NIST Special Publications 800-3, 800-18 and 800-47, and
- (ix) identify the types of positions that require screening pursuant to Section 3.12, the required rigor of such screening by type of position, and the criteria by which Domestic Communications Companies will accept or reject screened persons ("Screened Personnel").

3 10 Security Officer Responsibilities and Duties The Head of Global Security of New GX, or a designee in a direct reporting relationship with the Head of Global Security, shall serve as the Security Officer with the primary responsibility for ensuring compliance with the Domestic Communications Companies' obligations under Article 3 and Sections 5 2, 5 5, 5 6, 5 7, 5 11, and 5 12 of this Agreement, and shall have the qualifications set forth in Section 3 13 Within thirty (30) days after the Effective Date, New GX shall notify the DOJ, FBI, DOD and DHS of the identity of the Security Officer

3 11 Disclosure of Protected Data In carrying out the responsibilities set forth in Section 3 10, the Security Officer shall not directly or indirectly disclose information concerning Lawful U.S. Process, Classified Information, Sensitive Information, or Controlled Unclassified Information to any third party or to any officer, director, shareholder, employee, agent, or contractor of New GX or any Domestic Communications Company, including those who serve in a supervisory, managerial or officer role with respect to the Security Officer, except to a Security Director (i) consistent with the Security Officer's or the Security Committee's duties or (ii) to the extent required to comply with this Agreement, unless disclosure has been approved by prior written consent obtained from the FBI, DOJ, DOD or DHS or there is an official need for disclosure of the information in order to fulfill an obligation consistent with the purpose for which the information is collected or maintained

3 12 Screening of Personnel Each Domestic Communications Company shall implement a thorough screening process through a reputable third-party to ensure that all personnel whose position involves access to the Domestic Communications Infrastructure that enables those persons to monitor the content of Wire or Electronic Communications (including in electronic storage) or to have access to Transactional Data, Call Associated Data or Subscriber Information, persons who have access to Sensitive Information, and security personnel meet personnel screening requirements agreed to by New GX, DOJ, the FBI, DOD and DHS The screening process undertaken pursuant to this Section shall follow the guidance to U.S. government agencies for screening civilian Federal employees in Executive Order 10450, and shall specifically include a background and financial investigation, an additional criminal record check, and a review of at least three references. Newly hired personnel will also be required to sign a non-disclosure agreement approved in advance by DOJ, FBI, DOD and DHS.

- (i) New GX shall consult with DOJ, the FBI, DOD and DHS on the screening procedures utilized by the reputable third party and shall provide to DOJ, FBI, DOD and DHS a list of the positions subject to screening New GX shall utilize the criteria identified pursuant to Section 3 9 (1x) to screen personnel, shall report the results of such screening on a regular basis to the Security Committee, and shall, upon request, provide to the investigations services of the DOJ, the FBI, DOD and DHS or, in the alternative, to the investigations service of OPM, all the information it collects in its screening process of each candidate Candidates for these positions shall be informed that the information collected during the screening process may be provided to the U.S. government, and the candidates shall consent to the sharing of this information with the U.S. government



- (ii) If the DOJ, the FBI, DOD or DHS so desires, it may on its own, or through OPM's investigations service, conduct further background checks for Screened Personnel. New GX will cooperate with any U.S. government agency undertaking any such further background checks.
- (iii) Individuals who are rejected by the DOJ, the FBI, DOD or DHS for the screening requirements agreed to pursuant to this Section 3.12 of this Agreement will not be hired or, if they have begun their employment, will be immediately removed from their positions or otherwise have their duties immediately modified so that they are no longer performing a function that would require screening under this Section. New GX will notify the DOJ, the FBI, DOD and DHS of the transfer, departure, or job modification of any individual rejected as a result of the screening conducted pursuant to this Section 3.12 of this Agreement within seven (7) days of such transfer or departure, and shall provide the DOJ, the FBI, DOD and DHS with the name, date of birth and social security number of such individual.
- (iv) New GX shall provide training programs to instruct Screened Personnel as to their obligations under the Agreement and the maintenance of their trustworthiness determination or requirements otherwise agreed. New GX shall monitor on a regular basis the status of Screened Personnel, and shall remove personnel who no longer meet the Screened Personnel requirements.
- (v) New GX shall maintain records relating to the status of Screened Personnel, and shall provide these records, upon request, to the DOJ, FBI, DOD, DHS or any third party auditor appointed under the terms of Section 5.8 below.

3.13 Qualification of Principal Network and Security Officers. New GX shall employ a Head of Network Operations and a Head of Global Security for Domestic Communications Companies. Within thirty (30) days after the Effective Date, New GX shall notify the DOJ, FBI, DOD and DHS of the identities of the Head of Network Operations and the Head of Global Security. The Head of Network Operations and the Head of Global Security, and any designee of the Head of Global Security who serves as the Security Officer under Section 3.10, shall be resident citizens of the United States who, if not already in possession of U.S. security clearances, shall apply for U.S. security clearances pursuant to Executive Order 12968 immediately upon their appointment; who are subject to the screening requirements of Section 3.12 of this Agreement; and whose appointment to the position is not objected to by the DOJ, the FBI, DOD and DHS within ten (10) days of receiving notice thereof. If the Head of Network Operations, the Head of Global Security, or any designee of the Head of Global Security who serves as the Security Officer under Section 3.10, does not already possess a U.S. security clearance, he or she may nevertheless serve in that position, subject to DOJ, FBI, DOD and DHS approval, pursuant to an interim security clearance. New GX shall have the right to remove the Head of Network Operations or the Head of Global Security at any time and to appoint a replacement, subject to the terms of this Section. New GX shall promptly appoint a person who meets the qualifications of this Section to fill any such vacancy, and shall promptly notify the DOJ, FBI, DOD, and DHS in writing of such appointment. In no event shall a vacancy for the position of Head of

Network Operations or Head of Global Security exist for a period of more than ninety (90) days before New GX appoints a qualified candidate to fill such vacancy

3.14 Qualification of General Counsel and Head of Human Resources. Within thirty (30) days after the Effective Date, New GX shall notify DOJ, FBI, DHS and DOD of the identities of the Human Resources executive responsible for hiring and screening and the General Counsel. The Human Resources executive responsible for hiring and screening and the General Counsel shall be resident citizens of the United States who, if not already in possession of U.S. security clearances, shall apply for U.S. security clearances pursuant to Executive Order 12968 immediately upon their appointment, who are subject to the screening requirements of Section 3.12 of this Agreement, and whose appointment to the position is not objected to by the DOJ, the FBI, DOD or DHS within ten (10) days of receiving notice thereof. If the Human Resources executive responsible for hiring and screening or the General Counsel does not already possess a U.S. security clearance, he or she may nevertheless serve in that position, subject to DOJ, FBI, DOD and DHS approval, pursuant to an interim security clearance. New GX shall have the right to remove the Human Resources executive responsible for hiring and screening and the General Counsel at any time and to appoint a replacement, subject to the terms of this Section. New GX shall promptly appoint a person who meets the qualifications of this Section to fill any such vacancy, and shall promptly notify the DOJ, FBI, DOD, and DHS in writing of such appointment. In no event shall a vacancy for the position of Human Resources executive responsible for hiring and screening or General Counsel exist for a period of more than ninety (90) days before New GX appoints a qualified candidate to fill such vacancy.

3.15. Establishment of Security Committee of New GX Board. The New GX Board shall establish a Security Committee to oversee security matters within Domestic Communications Companies. The Security Committee shall be comprised solely of directors ("Security Directors") who are U.S. citizens, who, if not already in possession of U.S. security clearances, shall apply for U.S. security clearances pursuant to Executive Order 12968 immediately upon their appointment to the Security Committee, and who satisfy the independent director requirements of the New York Stock Exchange. If a Security Director does not already possess a U.S. security clearance, he or she may nevertheless serve as Security Director, subject to DOJ, FBI, DOD and DHS approval, pursuant to an interim security clearance. The Security Committee shall supervise and report to the full New GX Board on all matters related to security, including implementation of this Agreement, consistent with their obligation to keep such information confidential. To perform its function, the Security Committee shall, among other things, receive reports from the Head of Global Security on New GX's compliance with this Agreement, and also shall receive a summary of any report issued pursuant to this Agreement, including reports made in connection with audits conducted pursuant to Section 5.8 of this Agreement and the annual report on compliance issued pursuant to Section 5.11 of this Agreement. The Security Committee shall, in turn, provide general reporting to the full New GX Board on New GX's compliance with this Agreement.

3.16 Number and Notice of Appointment of Security Directors. Subject to Section 3.20 below, fifty (50) percent of the members of the New GX Board nominated by ST Telemedia and elected to the New GX Board shall be Security Directors. Notice of the

proposed appointment of a Security Director shall be provided in writing to the DOJ, FBI, DOD and DHS by New GX. The DOJ, FBI, DOD and DHS shall have the opportunity to review and disapprove the appointment of a Security Director within thirty (30) days of receiving notice of the proposed appointment. If the DOJ, FBI, DOD or DHS objects to the appointment of an individual as Security Director within the 30-day timeframe, the appointment of that individual shall be rescinded and a different candidate shall be appointed.

3.17 Approval of Acquisition. Acquiring or upgrading network hardware (*e.g.*, routers, switches, servers and network transmission capability) and network operating systems software requires prior approval of a Security Director, unless subject to other procedures pursuant to a policy to be negotiated with DHS. That policy may provide for simplified procedures for non-sensitive acquisitions and upgrades (*e.g.*, vetting by the Head of Network Operations).

3.18 Participation of Security Directors in Committees of the Board of New GX. A quorum for a meeting of the New GX Board or any committee of the New GX Board shall require at least one Security Director, unless the issues addressed at such meeting in no respect address or affect the obligations of New GX under this Agreement. In the event that the New GX Board or any committee of the New GX Board must address at a meeting, for reasons of exigent circumstances, an issue related to or affecting the obligations of New GX under this Agreement, and all Security Director positions are vacant at the time of such a meeting, the absence of the Security Director will not prevent the formation of a quorum provided that the Security Officer of New GX attends the meeting.

3.19 Attendance of Security Directors at Board Meetings of Domestic Communications Companies. A meeting of the board of a Domestic Communications Company or of a board committee of a Domestic Communications Company shall not occur without a Security Director in attendance, whether as a member or as an observer, unless the issues addressed at such meeting in no respect address or affect the obligations of the Domestic Communications Company under this Agreement. In the event that the board of a Domestic Communications Company or a board committee of a Domestic Communications Company must address at a meeting, for reasons of exigent circumstances, an issue related to or affecting the obligations of the Domestic Communications Company under this Agreement, and all Security Director positions are vacant at the time of such a meeting, the absence of the Security Director will not prevent the meeting provided that the Security Officer of New GX attends the meeting.

3.20 Removal of Security Directors. Any Security Director may be removed for any reason permitted by the provisions of applicable law or under the charter of New GX, provided that

- (i) the removal of a Security Director shall not become effective until that Security Director, DOJ, the FBI, DOD and DHS have received written notification, a successor who is qualified to become a Security Director within the terms of this Agreement is selected, DOJ, the FBI, DOD and DHS receive written notice of such selection under the terms of this Agreement, and DOJ, the FBI, DOD or

DHS do not object to the proposed Security Director within thirty (30) days of such notice, and

- (ii) notification to DOJ, the FBI, DOD and DHS of the removal of a Security Director shall be the responsibility of the General Counsel of New GX

Notwithstanding the foregoing, however, if immediate removal of any Security Director is deemed necessary to prevent actual or possible violation of any statute or regulation or actual or possible damage to New GX, the Security Director may be temporarily suspended, pending written notification to the FBI, DOJ, DOD and DHS, and removed upon the approval of the removal by the FBI, DOJ, DOD and DHS. The written notification to DOJ, FBI, DOD and DHS shall set forth the reasons for the removal if such reasons are related to the performance of this Agreement. In the event of any vacancy in the position of Security Director, however occurring, New GX will give prompt written notice of such vacancy to DOJ, the FBI, DOD and DHS through the General Counsel of New GX, or if that position is vacant, through the Chief Operating Officer of New GX. New GX shall promptly nominate a person who meets the qualifications in Section 3.15 to fill such vacancy, and shall promptly notify DOJ, the FBI, DOD and DHS in writing of such nomination. In no event shall a vacancy for the position of Security Director exist for a period of more than ninety (90) days before New GX nominates a qualified candidate to fill such vacancy.

3.21 Indemnification of Security Directors. New GX shall indemnify and hold harmless each Security Director from any and all claims arising from, or in any way connected to, his or her performance as a Security Director under the Agreement except for his or her own individual gross negligence or willful misconduct. New GX shall advance fees and costs incurred in connection with the defense of such claim. New GX may purchase insurance to cover this indemnification.

3.22 Operational Control of New GX Network. Except to the extent and under conditions concurred in by the FBI, DOJ, DOD and DHS in writing, operational control of the Domestic Communications Infrastructure will be restricted to the New GX Network Operating Centers located in the United States.

3.23 Security Standards and Practices, and Consultations with U.S. Government. Domestic Communications Companies will maintain or exceed security standards and practices utilized within the U.S. telecommunications industry and will consult with the DOJ and other appropriate U.S. government agencies on steps to maintain or exceed such standards and practices.

3.24 Notice of Obligations. Domestic Communications Companies shall instruct appropriate officials, employees, contractors, and agents as to the security restrictions and safeguards imposed by this Agreement, including the reporting requirements in Sections 5.5, 5.6, and 5.7 of this Agreement, and shall issue periodic reminders to them of such obligations.

3.25 Access to Classified, Controlled Unclassified, or Sensitive Information. Nothing contained in this Agreement shall limit or affect the authority of a U.S. government agency

to deny, limit or revoke Domestic Communications Companies' access to Classified, Controlled Unclassified, and Sensitive Information under that agency's jurisdiction.

#### ARTICLE 4: DISPUTES

4.1 Informal Resolution The Parties shall use their best efforts to resolve any disagreements that may arise under this Agreement. Disagreements shall be addressed, in the first instance, at the staff level by the Parties' designated representatives. Any disagreement that has not been resolved at that level shall be submitted promptly to the General Counsel of New GX, the General Counsel of the FBI, and the Deputy Attorney General, Criminal Division, DOJ, the General Counsel of DOD, and the General Counsel of DHS or their designees, unless the FBI, DOJ, DOD or DHS believes that important national interests can be protected, or a Domestic Communications Company believes that its paramount commercial interests can be resolved, only by resorting to the measures set forth in Section 4.2 of this Agreement. If, after meeting with higher authorized officials, any of the Parties determines that further negotiation would be fruitless, then that Party may resort to the remedies set forth in Section 4.2 of this Agreement. If resolution of a disagreement requires access to Classified Information, the Parties shall designate a person or persons possessing the appropriate security clearances for the purpose of resolving that disagreement.

4.2 Enforcement of Agreement Subject to Section 4.1 of this Agreement, if any of the Parties believes that any other of the Parties has breached or is about to breach this Agreement, that Party may bring an action against the other Party for appropriate judicial relief. Nothing in this Agreement shall limit or affect the right of a U.S. government agency to

- (i) require that the Party or Parties believed to have breached, or about to breach, this Agreement cure such breach within thirty (30) days upon receiving written notice of such breach,
- (ii) request that the FCC modify, condition, revoke, cancel or render null and void any license, permit, or other authorization granted or given by the FCC to Domestic Communications Companies, or request that the FCC impose any other appropriate sanction, including but not limited to a forfeiture or other monetary penalty, against Domestic Communications Companies,
- (iii) seek civil sanctions for any violation by New GX or Domestic Communications Companies of any U.S. law or regulation or term of this Agreement;
- (iv) pursue criminal sanctions against New GX or Domestic Communications Companies, or any director, officer, employee, representative, or agent of Domestic Communications Companies, or against any other person or entity, for violations of the criminal laws of the United States; or
- (v) seek suspension or debarment of New GX or Domestic Communications Companies from eligibility for contracting with the U.S. government.